RSA SecurID®
Setup guide: Server Installation

DISCLAIMER

This documentation is intended for informational purposes only. These guides reflect the NASA SEWP Security Center experiences with this product. These guides are independent and are to be used as a reference to setting up the RSA SecurID® product. There are no express or implied warranties regarding the veracity of the information provided. Please read the RSA documentation for complete product information.

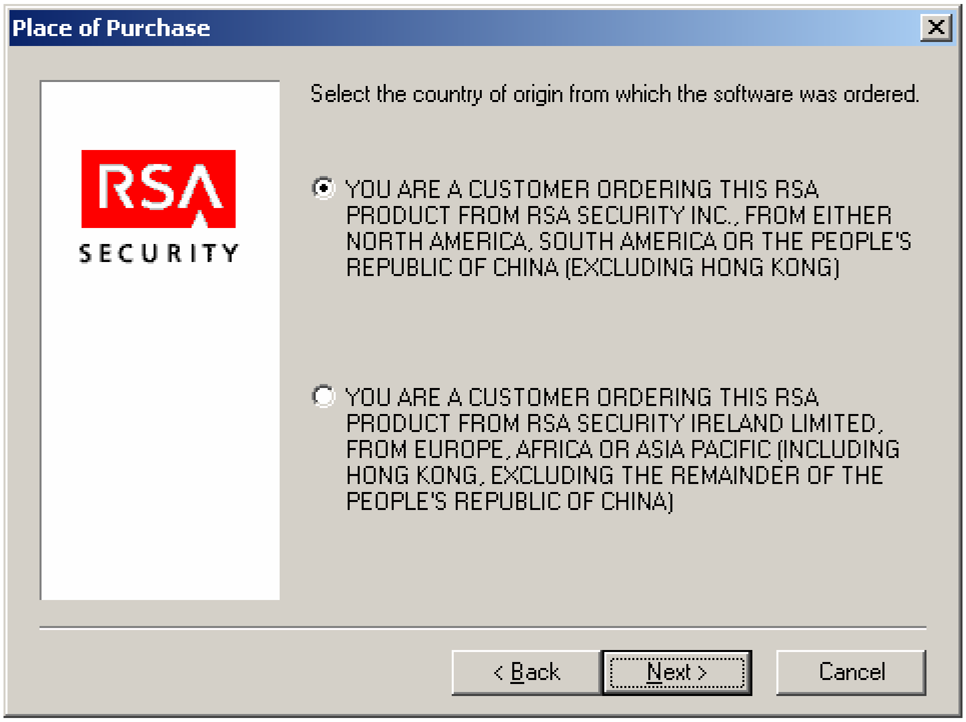
This guide is to help a system administrator setup RSA ACE Server installation to the IT environment. Note that the setup guide is another layout to the provided documentation with the CD or in a download. The guide is designed for basic setup and any specific protection or requirements are not reflected in this guide. For example, the system admin must specify the length of a PIN, determine whether a user generates the PIN, and decide if passwords are allowed, etc.

The first part will be setting up the server; from install to configuration. The second part is setting up for the Agent host. It is encouraged to read the provided documentation that came with the CD or download.

Server installation:

Note: This is for ACE Server 6.0 (Authentication Manager 6.0).

1. **Open the Ace server folder > aceserv > click on setup.exe**
    a. *(based on download) as601_win > aceserv > windows > setup.exe*
2. **Go past the welcome screen**
3. **Choose the area of purchase (my case North America) > Next**

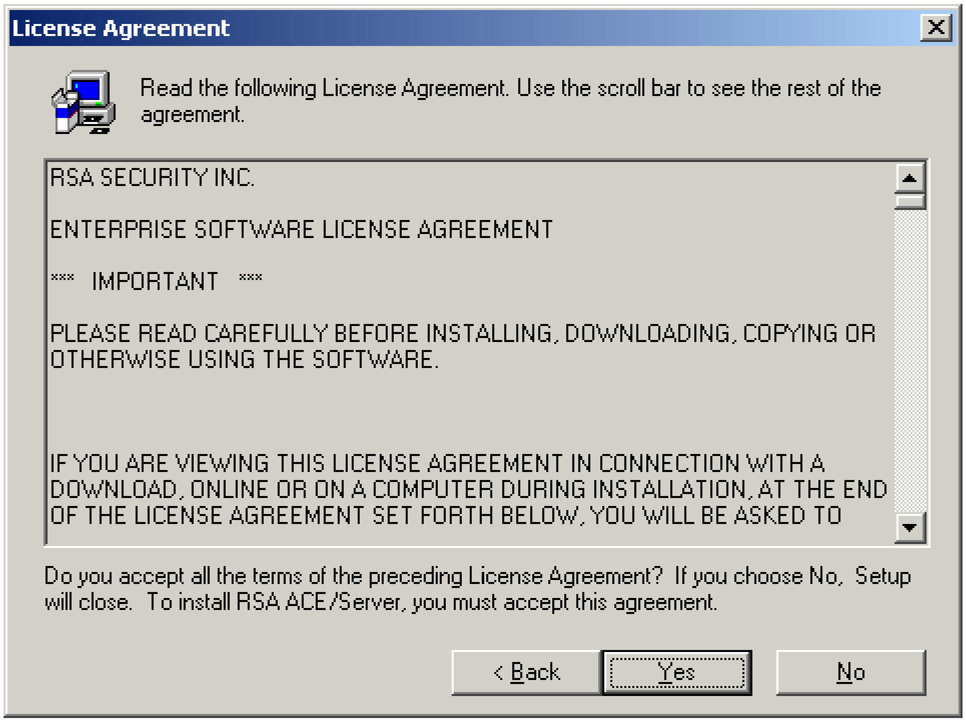


Select the country of origin from which the software was ordered.

● YOU ARE A CUSTOMER ORDERING THIS RSA PRODUCT FROM RSA SECURITY INC., FROM EITHER NORTH AMERICA, SOUTH AMERICA OR THE PEOPLE'S REPUBLIC OF CHINA (EXCLUDING HONG KONG)

○ YOU ARE A CUSTOMER ORDERING THIS RSA PRODUCT FROM RSA SECURITY IRELAND LIMITED, FROM EUROPE, AFRICA OR ASIA PACIFIC (INCLUDING HONG KONG, EXCLUDING THE REMAINDER OF THE PEOPLE'S REPUBLIC OF CHINA)

4. **Read and Agree to the License Agreement > Yes**



Read the following License Agreement. Use the scroll bar to see the rest of the agreement.

RSA SECURITY INC.

ENTERPRISE SOFTWARE LICENSE AGREEMENT

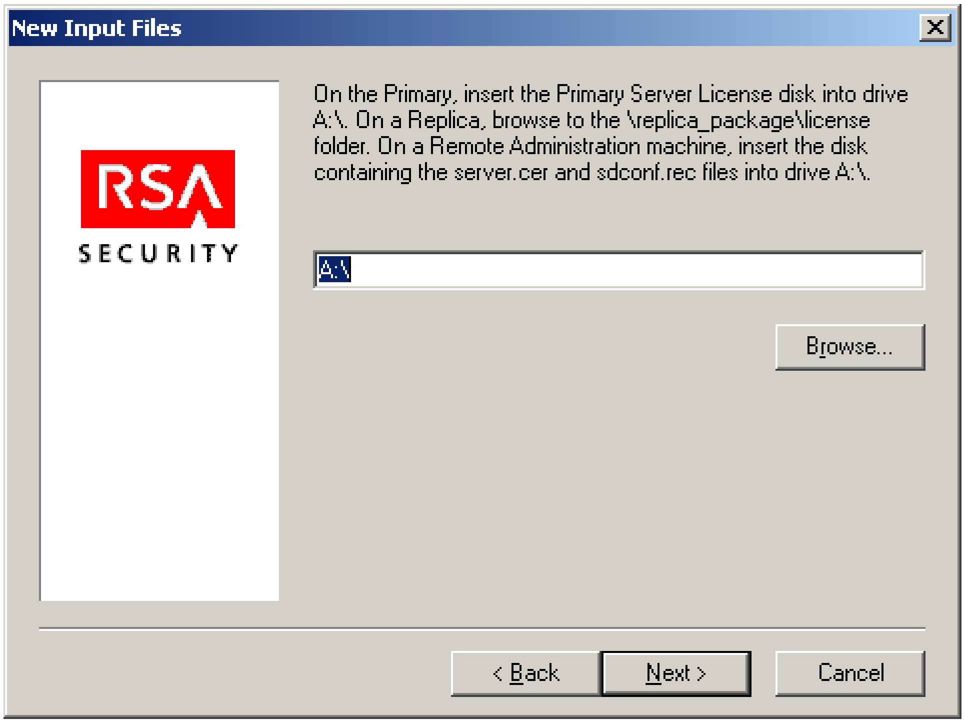
*** IMPORTANT ***

PLEASE READ CAREFULLY BEFORE INSTALLING, DOWNLOADING, COPYING OR OTHERWISE USING THE SOFTWARE.

IF YOU ARE VIEWING THIS LICENSE AGREEMENT IN CONNECTION WITH A DOWNLOAD, ONLINE OR ON A COMPUTER DURING INSTALLATION, AT THE END OF THE LICENSE AGREEMENT SET FORTH BELOW, YOU WILL BE ASKED TO

Do you accept all the terms of the preceding License Agreement? If you choose No, Setup will close. To install RSA ACE/Server, you must accept this agreement.

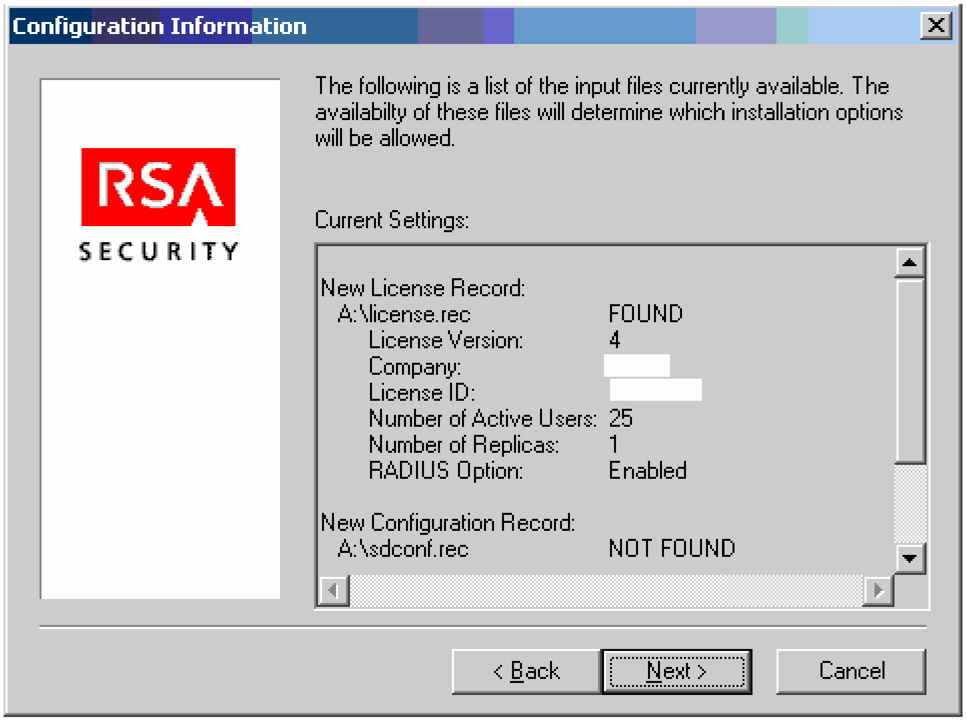
5. Locate your License file on disk. It should be with your purchased package or provided with download. Note this is also the same license on a disk if you have an older version of the ACE Server. In this case it came with the 5.1 package. The license file is the same no matter what version of The ACE Server you are using. > Next



On the Primary, insert the Primary Server License disk into drive A:\. On a Replica, browse to the \replica_package\license folder. On a Remote Administration machine, insert the disk containing the server.cer and sdconf.rec files into drive A:\.

A:\

6. Review the information to make sure it's correct > Next (All white boxes will be the company's information and will be filled in during install)

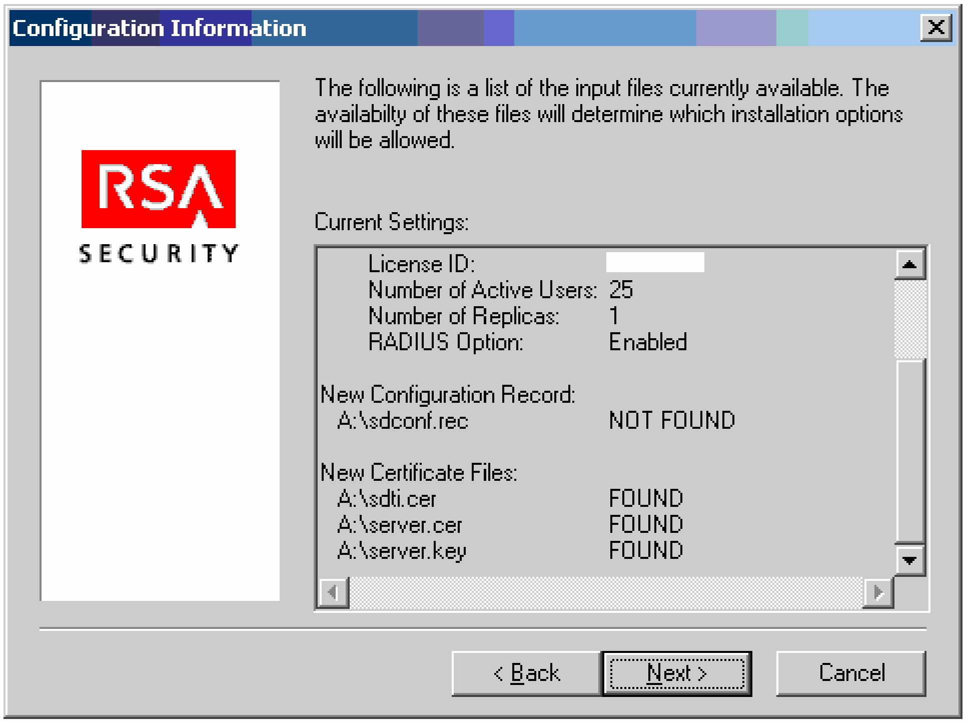


The following is a list of the input files currently available. The availabilty of these files will determine which installation options will be allowed.

Current Settings:

```
New License Record:
  A:\license.rec                FOUND
      License Version:          4
      Company:
      License ID:
      Number of Active Users:  25
      Number of Replicas:       1
      RADIUS Option:            Enabled

New Configuration Record:
  A:\sdconf.rec                 NOT FOUND
```



The following is a list of the input files currently available. The availabilty of these files will determine which installation options will be allowed.

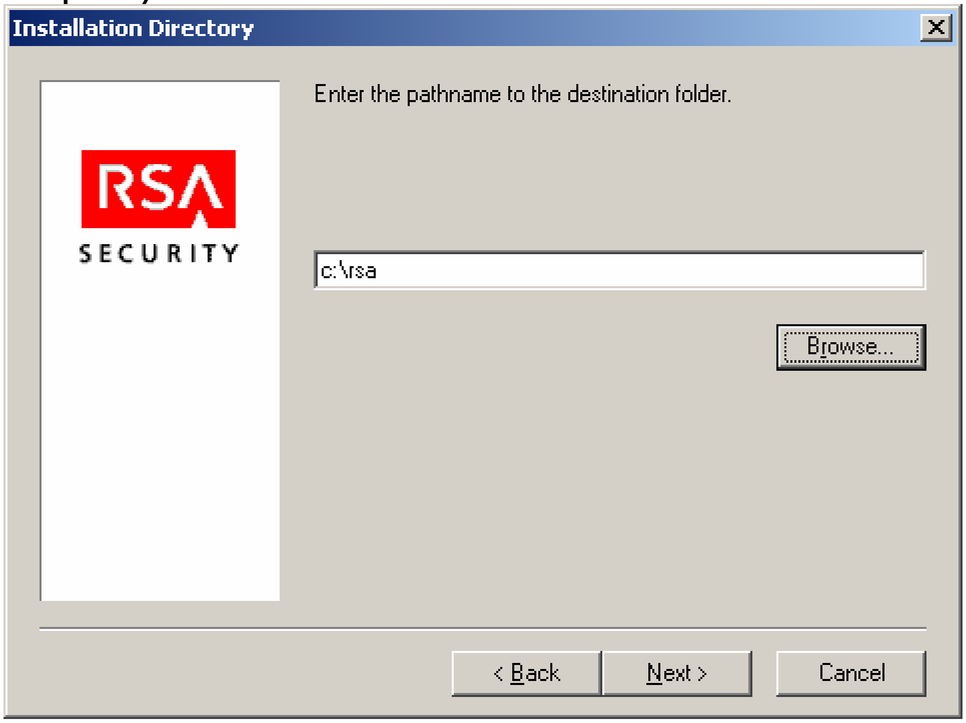
Current Settings:

```
      License ID:
      Number of Active Users:  25
      Number of Replicas:       1
      RADIUS Option:            Enabled

New Configuration Record:
  A:\sdconf.rec                 NOT FOUND

New Certificate Files:
  A:\sdti.cer                   FOUND
  A:\server.cer                 FOUND
  A:\server.key                 FOUND
```

7. Specify the location to install to. Note a folder will automatically be made. (I made an extra directory name RSA to store the installed components, you do not have to that nor is it required.)

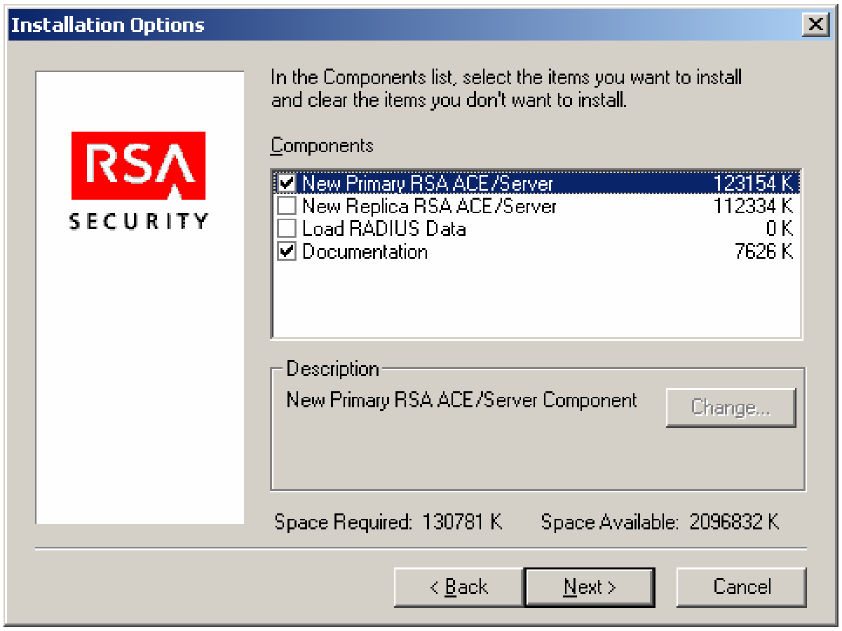


Installation Directory

Enter the pathname to the destination folder.

c:\rsa

8. Check the New Primary RSA ACE/Server and Documentation. (Note this is not the replica server. Leave unchecked you will check this when creating a replica) > Next



Installation Options

In the Components list, select the items you want to install and clear the items you don't want to install.

Components

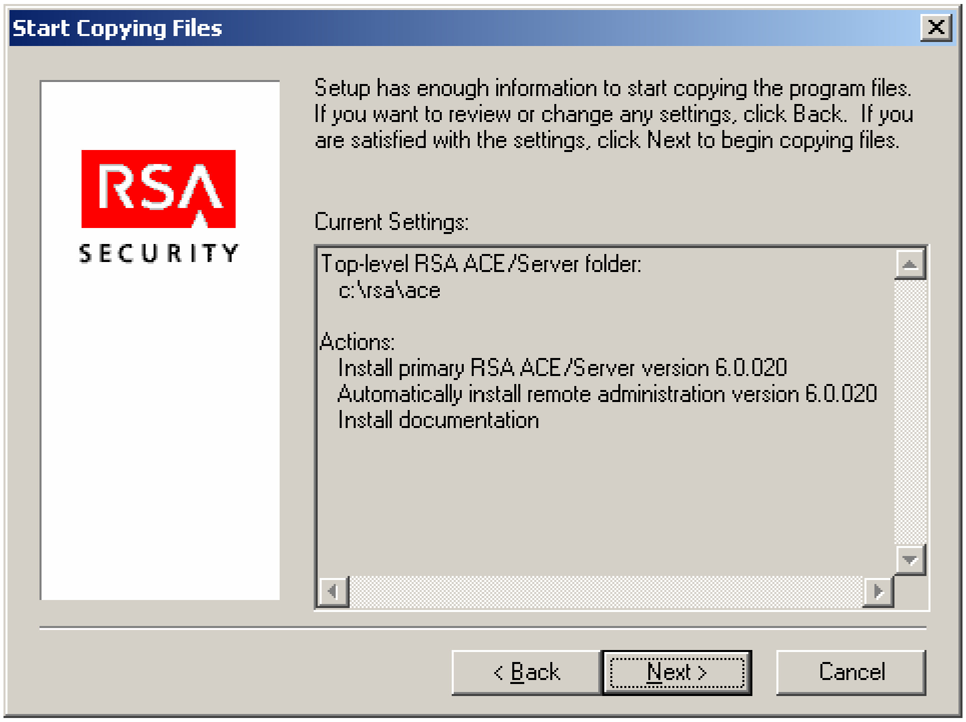
☑ New Primary RSA ACE/Server	123154 K
□ New Replica RSA ACE/Server	112334 K
□ Load RADIUS Data	0 K
☑ Documentation	7626 K

Description

New Primary RSA ACE/Server Component

Space Required: 130781 K Space Available: 2096832 K

9. Make sure information is correct > Next



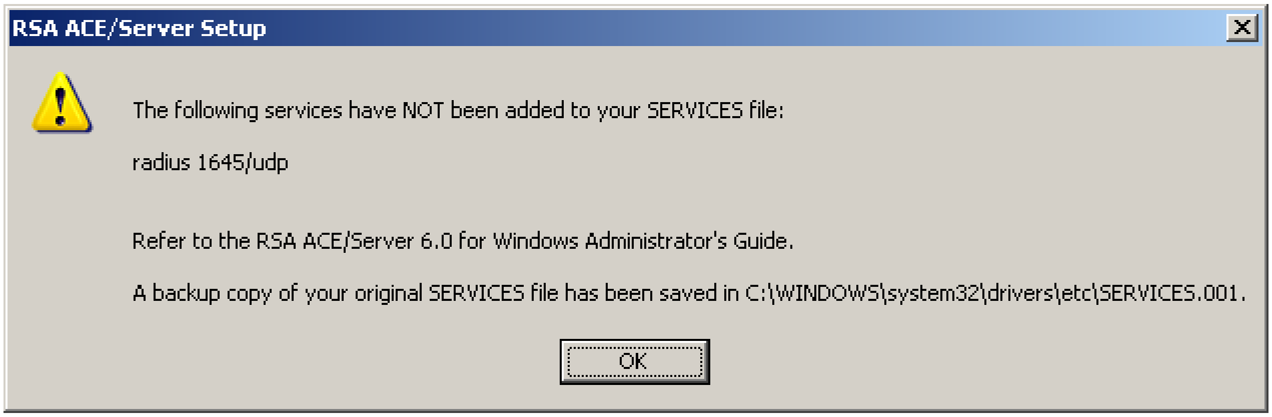
Setup has enough information to start copying the program files. If you want to review or change any settings, click Back. If you are satisfied with the settings, click Next to begin copying files.

Current Settings:

```
Top-level RSA ACE/Server folder:
   c:\rsa\ace

Actions:
   Install primary RSA ACE/Server version 6.0.020
   Automatically install remote administration version 6.0.020
   Install documentation
```

10. Note you can ignore this popup because in this setup we did not install the RADIUS service. This popup will not display if you decide to install the RADIUS service. Click OK



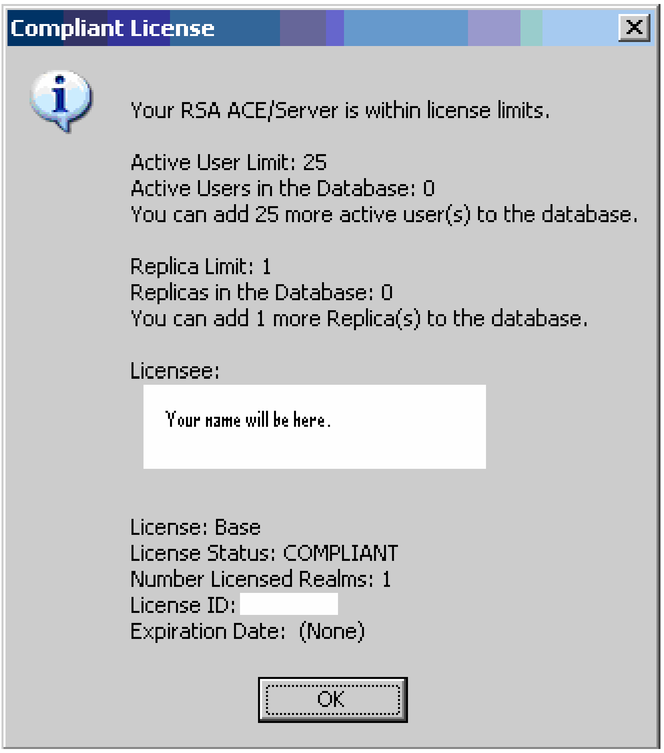
The following services have NOT been added to your SERVICES file:

radius 1645/udp

Refer to the RSA ACE/Server 6.0 for Windows Administrator's Guide.

A backup copy of your original SERVICES file has been saved in C:\WINDOWS\system32\drivers\etc\SERVICES.001.

11. Review the information of your Installation > OK



Compliant License

Your RSA ACE/Server is within license limits.

Active User Limit: 25
Active Users in the Database: 0
You can add 25 more active user(s) to the database.

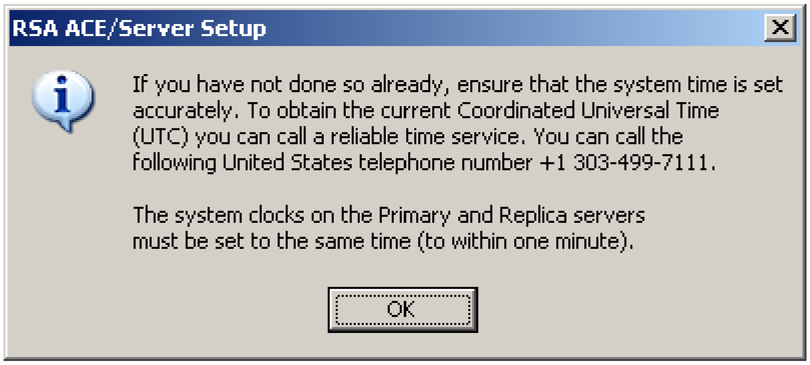
Replica Limit: 1
Replicas in the Database: 0
You can add 1 more Replica(s) to the database.

Licensee:

Your name will be here.

License: Base
License Status: COMPLIANT
Number Licensed Realms: 1
License ID:
Expiration Date: (None)

12. Follow the direction on screen > Ok

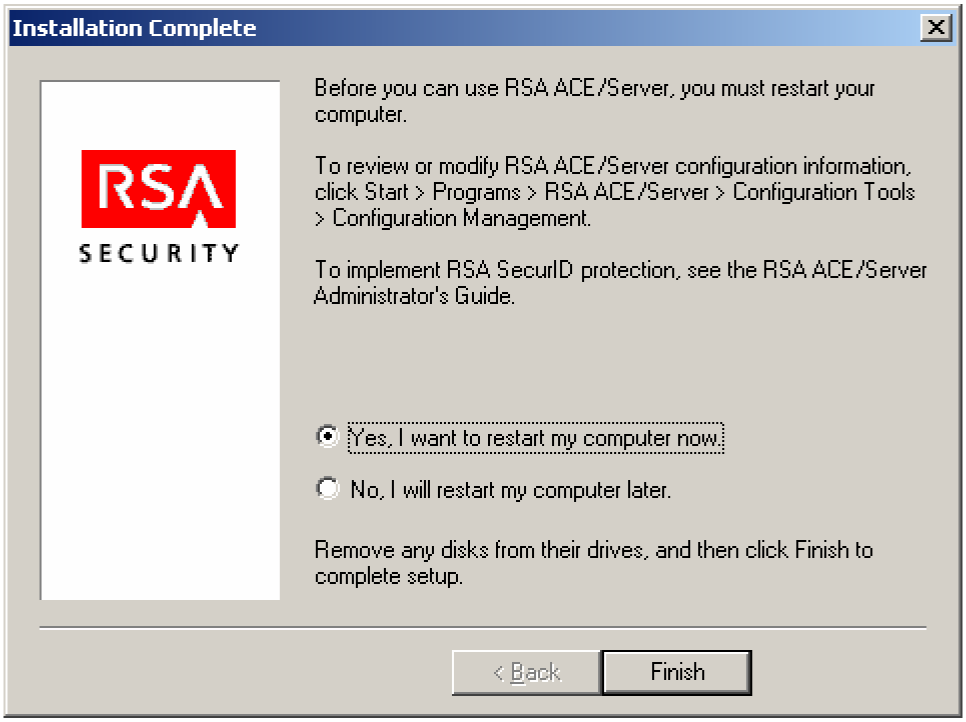


RSA ACE/Server Setup

If you have not done so already, ensure that the system time is set accurately. To obtain the current Coordinated Universal Time (UTC) you can call a reliable time service. You can call the following United States telephone number +1 303-499-7111.

The system clocks on the Primary and Replica servers must be set to the same time (to within one minute).

13. Restart computer > Finish



Before you can use RSA ACE/Server, you must restart your computer.

To review or modify RSA ACE/Server configuration information, click Start > Programs > RSA ACE/Server > Configuration Tools > Configuration Management.

To implement RSA SecurID protection, see the RSA ACE/Server Administrator's Guide.

● Yes, I want to restart my computer now.

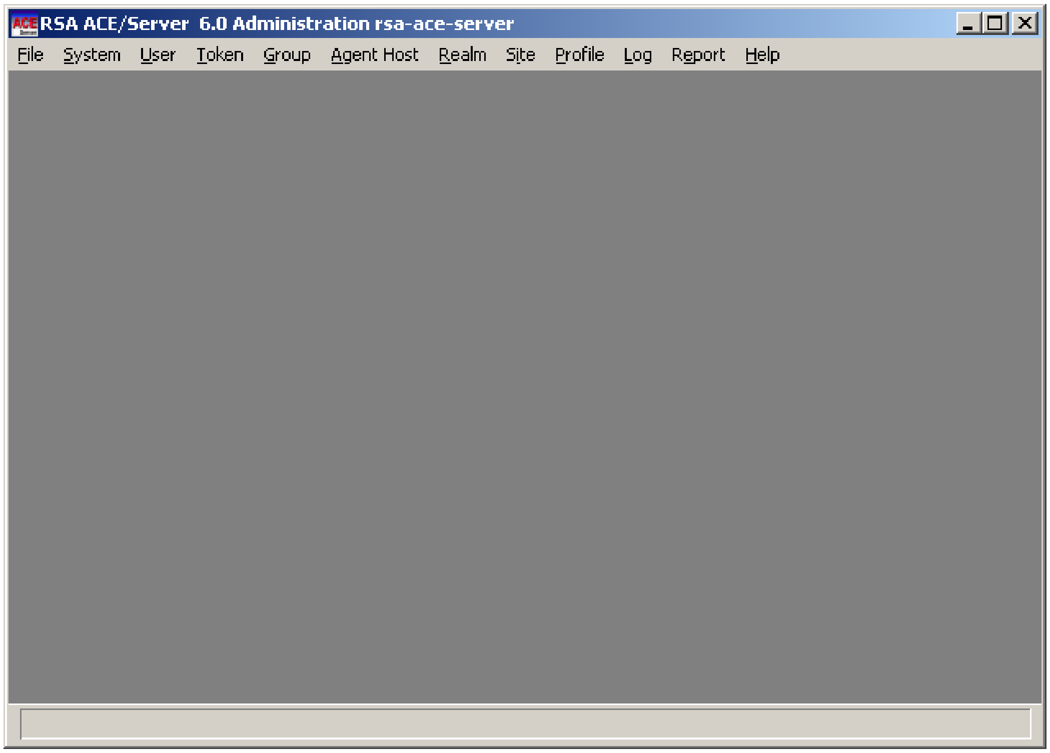
○ No, I will restart my computer later.

Remove any disks from their drives, and then click Finish to complete setup.

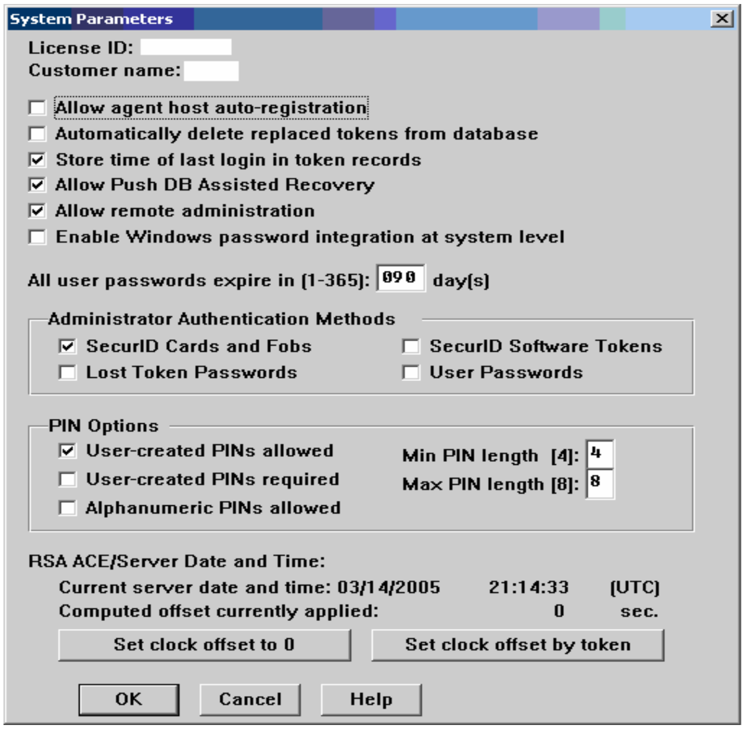
Things to do after install: (To ensure local authentication and proper agent install)

Now that the server has been installed, the next step is to configure the RSA ACE Server. It is recommended to configure the server at this point (after install) because it will be needed later when establishing connection with agents.

1. **Open the Ace server console host manager**
   - **a.** Log in as administrator: Click Start > All Programs > RSA ACE Server > Database Administration – Host Mode


RSA ACE/Server 6.0 Administration rsa-ace-server
File System User Token Group Agent Host Realm Site Profile Log Report Help

2. **Configure System: On tool bar click System > System Configuration > Edit System parameters**


System Parameters

License ID:
Customer name:

☐ Allow agent host auto-registration
☐ Automatically delete replaced tokens from database
☑ Store time of last login in token records
☑ Allow Push DB Assisted Recovery
☑ Allow remote administration
☐ Enable Windows password integration at system level

All user passwords expire in (1-365): 090 day(s)

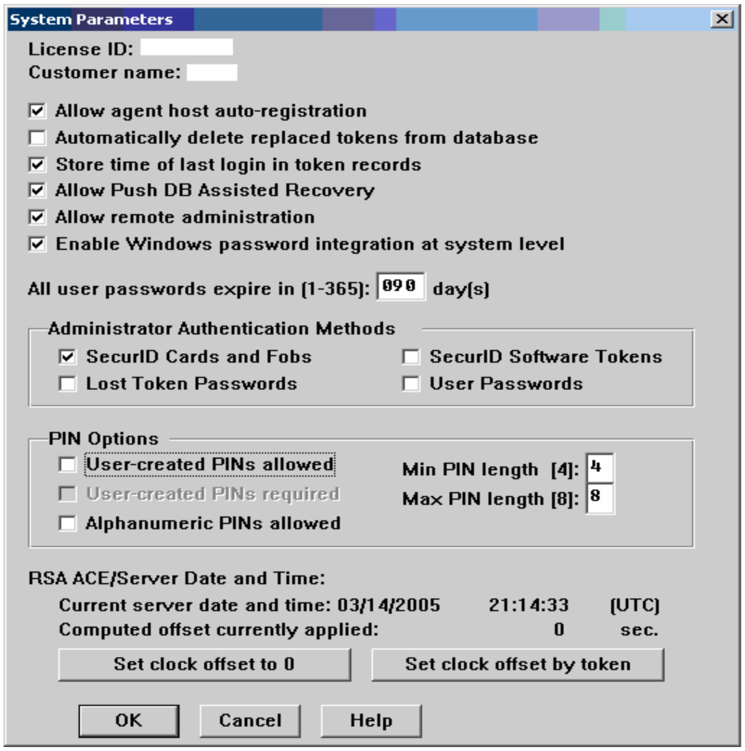
Administrator Authentication Methods
☑ SecurID Cards and Fobs
☐ Lost Token Passwords
☐ SecurID Software Tokens
☐ User Passwords

PIN Options
☑ User-created PINs allowed
☐ User-created PINs required
☐ Alphanumeric PINs allowed
Min PIN length [4]: 4
Max PIN length [8]: 8

RSA ACE/Server Date and Time:
Current server date and time: 03/14/2005 21:14:33 (UTC)
Computed offset currently applied: 0 sec.

3. **Check the “Allow agent host auto-registration and Enable Windows password Integration at system level. Unclick User-created PINs allowed (may have user do**

that but chose not to in my case)



System Parameters

License ID:

Customer name:

☑ Allow agent host auto-registration

□ Automatically delete replaced tokens from database

☑ Store time of last login in token records

☑ Allow Push DB Assisted Recovery

☑ Allow remote administration

☑ Enable Windows password integration at system level

All user passwords expire in (1-365): 090 day(s)

Administrator Authentication Methods

☑ SecurID Cards and Fobs □ SecurID Software Tokens

□ Lost Token Passwords □ User Passwords

PIN Options

□ User-created PINs allowed

□ User-created PINs required

□ Alphanumeric PINs allowed

Min PIN length [4]: 4

Max PIN length [8]: 8

RSA ACE/Server Date and Time:

Current server date and time: 03/14/2005 21:14:33 (UTC)

Computed offset currently applied: 0 sec.

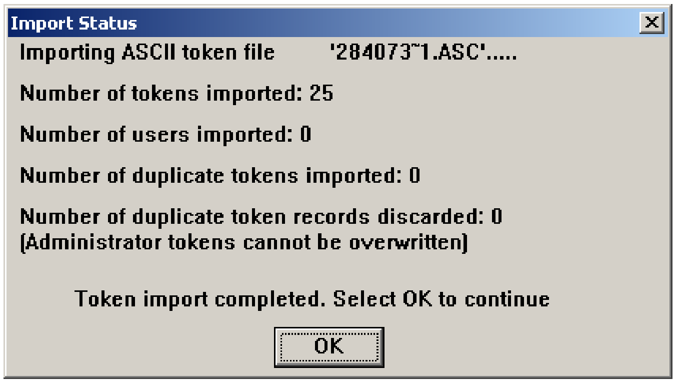
Importing Tokens: Populating database with tokens to deploy to the users.

This section of the setup guide focuses on importing the tokens that will need to distribute to the users/people of the organization. This section also assumes that you have gotten your tokens and have the proper token seed record to import the tokens. Depending on how the file came, you may need to decrypt the token seed record in order for the server to parse it.

Steps:

1. In the same view as configuring the server. Host Manager View. Click Token > Import Token > Pop up window appears to locate .ASC file or .XML file. Each or one should come with the package of bought tokens. Note that some files maybe encrypted and thus need to be decrypted first. Click on open ……Tokens are Imported unless a error occurred

2. OK



Importing ASCII token file '284073~1.ASC'.....

Number of tokens imported: 25

Number of users imported: 0

Number of duplicate tokens imported: 0

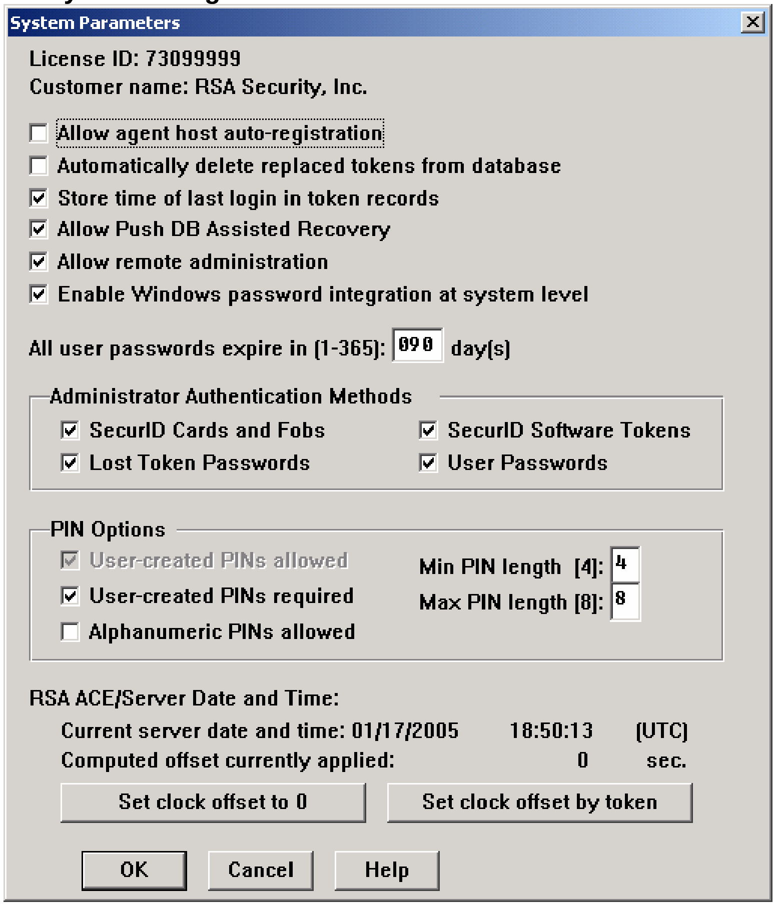
Number of duplicate token records discarded: 0
(Administrator tokens cannot be overwritten)

Token import completed. Select OK to continue

Configuring Password Integration and Offline Authentication on ACE/Server 6.0

Password integration is enabled at system level by default on ACE/Server:

RSA ACE/Server ------ > Administration ----->System Configuration ---> Edit System Parameters
Verify the settings:



License ID: 73099999
Customer name: RSA Security, Inc.

☐ Allow agent host auto-registration
☐ Automatically delete replaced tokens from database
☑ Store time of last login in token records
☑ Allow Push DB Assisted Recovery
☑ Allow remote administration
☑ Enable Windows password integration at system level

All user passwords expire in (1-365): 090 day(s)

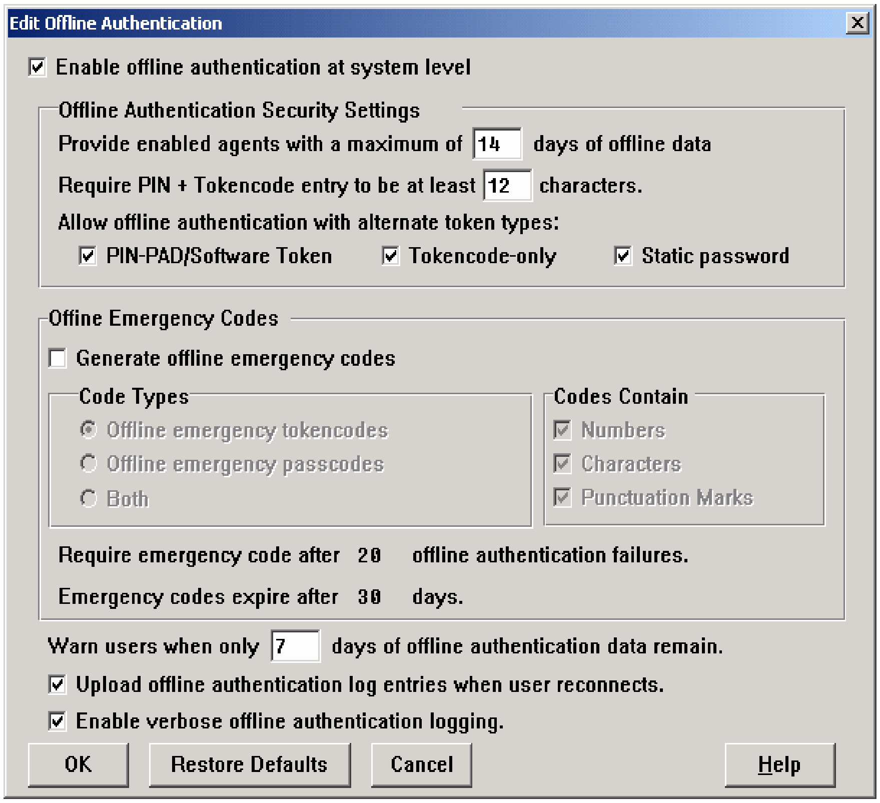
Administrator Authentication Methods
☑ SecurID Cards and Fobs ☑ SecurID Software Tokens
☑ Lost Token Passwords ☑ User Passwords

PIN Options
☑ User-created PINs allowed
☑ User-created PINs required
☐ Alphanumeric PINs allowed
Min PIN length [4]: 4
Max PIN length [8]: 8

RSA ACE/Server Date and Time:
Current server date and time: 01/17/2005 18:50:13 (UTC)
Computed offset currently applied: 0 sec.

Configuring Offline Authentication

Password integration must work in order to be able to accomplish offline authentication.
Administration --------> System Configuration ------ > Edit offline Auth Configuration
Offline Authentication is enabled by default at system level on ACE/Server.



Edit Offline Authentication

☑ Enable offline authentication at system level

Offline Authentication Security Settings

Provide enabled agents with a maximum of 14 days of offline data

Require PIN + Tokencode entry to be at least 12 characters.

Allow offline authentication with alternate token types:

☑ PIN-PAD/Software Token ☑ Tokencode-only ☑ Static password

Offine Emergency Codes

□ Generate offline emergency codes

Code Types

● Offline emergency tokencodes
○ Offline emergency passcodes
○ Both

Codes Contain

☑ Numbers
☑ Characters
☑ Punctuation Marks

Require emergency code after 20 offline authentication failures.

Emergency codes expire after 30 days.

Warn users when only 7 days of offline authentication data remain.

☑ Upload offline authentication log entries when user reconnects.

☑ Enable verbose offline authentication logging.

Configuring Offline Authentication at the System Level

Start ---→ Programs -→ RSA ACE/Server ------ > Database Administration ------ > System Configuration ----- >
Edit System Parameters ----- > Edit Offline Authentication…

To configure offline authentication parameters:

1**. In the Edit Offline Authentication dialog box, select Enable offline authentication at system level.**
This enables the other settings in the dialog box.

2. Specify Offline Authentication Security Settings.

a. Specify the number of days of offline authentication data that you want the Server to generate for enabled Agents.
The default is 14 days; the maximum value is 100 days.

b. Specify the length requirement for passcode entries (PIN combined with tokencode). A range of 8 to 16 characters is allowed. The default is 12 characters.

c. Specify the alternate token types with which offline authentication can be used. Available options are PIN-PAD, Tokencode-only, and Static password.

Important: If your users have already downloaded offline authentication data, and you then reduce the maximum number of days of data that can be downloaded, offline users will still be able to authenticate as long as they have offline data remaining. When users connect to the network, only then will the reduced number of offline logon days be downloaded. For optimum security, RSA Security recommends that the PIN + Tokencode setting be 12 characters (or more) in length. If your RSA SecurID tokens display six characters, for example, require your users to specify PINs that are at least six characters. RSA Security also recommends that you do not allow offline authentication with PIN-PAD, Tokencode-only, or Static password tokens.

3. Specify settings for Offline Emergency Codes.

a. To enable and define emergency access for your users when their computers are disconnected from the network, select Generate offline emergency codes.
b. Select the types of offline emergency codes that you want the Server to generate — Offline emergency tokencodes (for users who have misplaced their token), Offline emergency passcodes (for users who have forgotten their PIN and need a full passcode), or both.

Important: Because emergency passcodes enable authentication without a PIN, RSA Security recommends that you use emergency tokencodes instead. Users still must enter their PIN followed by the emergency tokencode to gain entry to their computers. Provide emergency passcodes only in situations where users have forgotten their PINs. In such cases, make sure you properly identify the users before providing them with emergency passcodes.

c. Specify the character types that offline emergency codes can contain — Numbers, Characters, and Punctuation Marks.
The default is to use all three character types, as this is the most secure.
d. Specify the number of failed offline authentication attempts before users must use an emergency code to gain entry to
their computers. The default is 20; the maximum is 100.
e. Specify the length of time (in days) after which emergency codes expire. The default is 30 days.

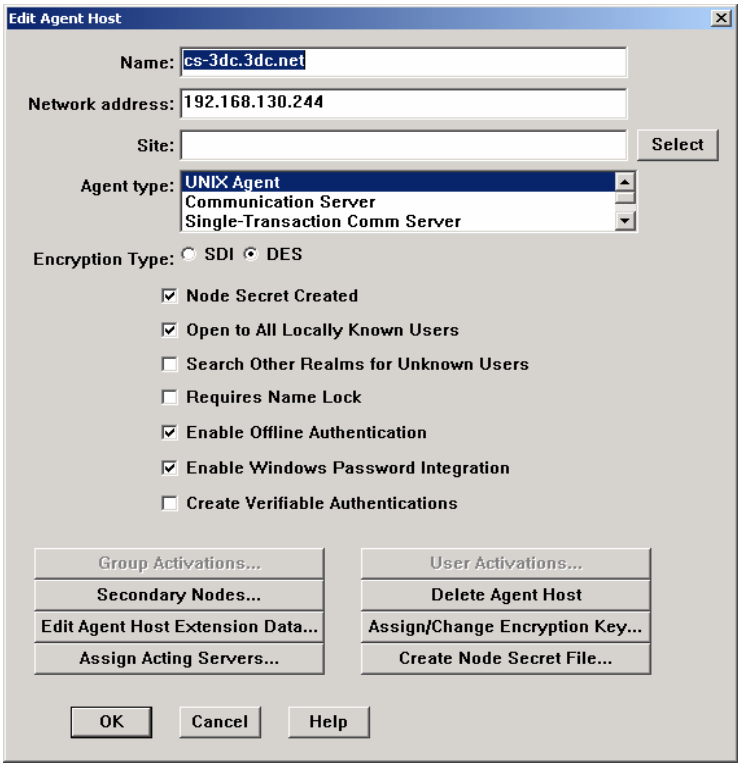
4. Specify the number of remaining days of offline authentication data that triggers a warning to users.

The default is 7 days. Offline computer users receive a message when they are running low on offline authentication data. Users have to reconnect to the company network to replenish their supply of offline logon days. If users completely run out of offline logon days, they may no longer be able to log in to their computers without help from their RSA ACE/Server administrator. For information about how users can reconnect and replenish their offline logon days, see the RSA ACE/Agent 6.0 Installation and Administration Guide.

5. If you want offline authentication events to be uploaded to the RSA ACE/Server's log database when users reconnect to the network, select Upload offline authentication log entries when user reconnects.

6. If you want detailed logging of offline authentication events, select Enable verbose offline authentication logging.
This will indicate a message on ACE/Server log after every 2 hours.

7. Click OK to accept the new offline authentication settings and close the dialog box. Alternatively, to restore the defaults, click Restore Defaults.
Password Integration and Offline Authentication at client level:
RSA ACE/Agent 6.0 must be installed on Agent host to utilize these features.
Edit Agent host:



Edit Agent Host

Name: cs-3dc.3dc.net

Network address: 192.168.130.244

Site:

Agent type: UNIX Agent
Communication Server
Single-Transaction Comm Server

Encryption Type: ○ SDI ● DES

☑ Node Secret Created

☑ Open to All Locally Known Users

□ Search Other Realms for Unknown Users

□ Requires Name Lock

☑ Enable Offline Authentication

☑ Enable Windows Password Integration

□ Create Verifiable Authentications

Note that offline authentication must be enabled at the system-level for this to work at Agent host level.
If the Agent Host is running version 6.0 RSA ACE/Agent for Windows software, select Enable Windows Password Integration. This specifies that users’ Windows passwords are automatically delivered to the Windows authentication engine when users authenticate with RSA SecurID. For this to work, Windows password integration must be enabled at the system-level.
Please refer to help topics on the above screen shot for other configuration details.